Research Proposal of the Thesis Entitled

Certain Investigations on Intrusion Detection in Wireless Sensor Networks Using Artificial Intelligence and Machine Learning Techniques

Submitted for the award of the Degree Of

Doctor of Philosophy

By

Divya Bhavani Mohan

Enrollment No: 202305001

Under the guidance of Dr. Prakash Arumugam

in the

Unitedworld Institute of Technology

Karnavati University, Gandhinagar

1. Introduction

Wireless Sensor Networks (WSNs) have gathered immense attention in the recent years as groundbreaking technology with numerous applications and significant transformative potential in many industries. The sensor nodes integrated in these networks are capable of detecting and recording the fluctuations in both the physical and environmental conditions related to temperature, pressure, sound, or motion. These sensors compile data through wireless communication and transmits the same to a centralized location for analysis.

2. Main Components of WSN:

- Sensors: These are the essential components that detects and measures the physical phenomena. They transform the detected phenomena into electrical signals for further processing.
- Actuators: These can activate a light or modify a valve by consuming the data collected from the sensors.
- Nodes: A node is a composition of a sensor, actuator, and possibly computational capabilities and communication interfaces.
- Gateway: This component permits the data transmission to a central server for additional analysis by connecting the WSN to external networks.
- Data Processing Unit: The data processing unit collects data obtained from the sensors and it is often situated at the gateway or a central server.
- Power Supply: The components of the WSN receives the power from batteries, solar panels, or other energy sources.

WSNs collect data through sensors, process it locally, and wirelessly transmit the data to other nodes or the base station. This decentralized technique enables efficient data collection and processing across wide areas or in demanding environments. The most important characteristics of Wireless Sensor Networks (WSNs) includes Self-organization - which enables the nodes in the network to be established independently and required connections are maintained; Scalability - where the network can be expanded whenever required by incorporating additional nodes; Energy efficiency – where the networks are designed to operate on limited power sources which will extended the network's life time; Fault tolerance – where the system should function normally even if there is malfunction in the nodes; Multi-hop communication – where the data may be transferred through multiple nodes to reach its anticipated terminals. Wireless Sensor Networks (WSNs) have applications across various sectors, consisting:

- Environmental monitoring: Observing climate and temperature patterns, measuring the pollution and assessing the pollutant concentration levels.
- Healthcare: Supervising patients' regular activities and assisting elderly people in their living environments.
- Industrial automation: Overseeing the entire production process and regulatory measures.

- Smart cities: Optimizing traffic management, collection of garbage through smart methodologies, and low power consumption for maximum efficiency.
- Agriculture: Employing and monitoring of the precision farming techniques and crop health monitoring.

WSNs may have multiple benefits but still face significant hurdles that include restricted power supply, limited power resources, security risks and data reliability issues. The current research focusses on framing of advanced techniques that includes enhancing the hardware designs, adapting high-end protocols, selection of advanced data processing methods and developing effective machine learning and deep learning models. The above techniques will help the network to be more stable by predicting the attacks accurately and increases the efficiency of the network at the time of intrusion detection.

As WSN technology advances, its impact in enhancing the Internet of Things (IoT) and intelligent environments is bound to increase exponentially, resulting in more efficient and sustainable solutions across variety of industries. This project seeks to create an innovative framework that incorporates a Machine Learning approach, augmented by an optimization algorithm, within a novel ensemble model to enhance network attack detection rates.

3. Key objectives

- Create innovative optimization techniques tailored for WSN limitations to boost the accuracy and efficiency of machine learning models in identification of attacks.
- Construct and implement ensemble models that combine multiple machine learning approaches to leverage their unique strengths and improve overall detection performance.
- Analyzing the usage and necessity of dimensionality reduction and feature selection methods to improve the input space for multiple machine learning models, considering diverse constraints imposed by wireless sensor network nodes.
- Formulating adaptive learning algorithms which aims at enhancing and sustaining operational efficiency in response to any type of intrusion attempts and fluctuating network conditions.
- Assessing the developed models using legitimate WSN datasets and simulated assault scenarios to substantiate their prowess in identifying array of attacks.
- Evaluating the trade-offs between various performance metrics, computing demands, and the energy consumption in order to ensure that the proposed strategies remain practical for WSN environments characterized with limited resources.

4. Review of Literature

This section presents the detailed literature review that synthesizes the key findings from various research articles related to this study. The table below summarizes the authors, the methodologies implemented, results obtained and research gaps.

Reference No.	Year	Authors	Methods Used	Results	Research Gap
[1]	2010	Ghalib Shah, Ather Ali - Year: 2010	- Use of MicaZ motes and custom sensor nodes for designing and implementing the WSN. - Evaluation of sensor capabilities and energy consumption. -Application of Passive Infrared (PIR) sensors for detection.	- The system achieved an 85% successful human detection rate. - Custom sensor nodes performed equally well as MicaZ motes. - Single hop communication distance ranged between 70-80 meters.	- Need for improved power and energy consumption solutions. - Development of robust WSN routing algorithms is necessary. - Security against over-the-air attacks requires enhancement. - Limitations of PIR sensors need addressing with better modules.
[2]	2011	Hossein Jadidoleslamy	- Utilization of Sensor-based Intrusion Detection Systems (SIDS) and Cluster-based Intrusion Detection Systems (CIDS). - Combination of signature and anomaly detection methods.	-Total average value of properties was 84.3%. -Processing properties scored the highest at 86.4%. -Technical properties averaged 84.2%. - Special and high-level properties averaged 85.8%. -Operational properties scored 81.2%.	- Limited exploration of dynamic hostile environments in WSNs. - Need for improved response scheduling and control mechanisms. - Lack of user-friendly interfaces for dynamic system reconfiguration. - Insufficient techniques for mobile node

					integration in WSNs.
[3]	2013	Emad Felemban	-Methods of aggregate alarms to minimize false alarms. -In-network processing for improved detection accuracy. -Logical Grid Routing Protocol for routing and localization. -Distributed algorithm for optimizing sensor node placement. -Multi-round approach for deploying sensor nodes.	- The paper surveys WSN applications in border surveillance. - It identifies challenges in deploying WSN for mission-critical applications. - The accuracy of detection and classification is emphasized. - Few real deployments of WSN in border protection are noted.	- Few attempts to address critical issues in border surveillance. - Limited research on WSN's application in mission-critical scenarios. -Challenges in processing power and communication reliability remain unaddressed. -Need for improved accuracy in detection and classification methods.
[4]	2019	Gebreyesus Gebrekiros, Gebremariam, J Panda, S Indu.	-Hybrid ML method for ID. -Spearman's rank correlation coefficient for feature selection. -Ensemble techniques: bagging, boosting, and stacking.	- The proposed system achieved 99.80% detection accuracy with NSL-KDD dataset. - 100% classification accuracy was achieved with UNSW_NB15 dataset. -99.46% average detection accuracy for routing attacks was reported.	- Limited studies on hierarchical WSN challenges and opportunities. - Need for optimal hybrid machine learning algorithm combinations. - Insufficient real-world WSN deployment evaluations. - Scalability issues in resource-constrained environments.

[5]	2024	Karthikeyan, D Manimegalai, Karthikeyan Rajagopal.	- Firefly Algorithm (FA) integrated with ML. - Classification using Support Vector Machine (SVM). - Parameter tuning using Grey Wolf Optimizer (GWO).	FA-ML achieved Accuracy - 99.29% Sensitivity - 98.12% Specificity - 99.59% F1-score - 96.23% AUC score 98.51%	- Existing methods lack efficiency in WSN-IoT intrusion detection. - Limited exploration of feature selection techniques for high-dimensional data. - Need for improved optimization algorithms in intrusion detection systems.
[6]	2023	Salim Salmi, Lahcen Oughdir	-CNN, DNN, RNN, CNN+RNN models. - Utilization of the WSN-DS dataset for training. - Implementation of dropout layers to prevent overfitting.	- CNN accuracy 98.75%. - DNN accuracy 97.07%. - CNN+RNN accuracy 96.84% - RNN accuracy of 96.50%.	- The paper does not address real-time detection challenges. - Limited exploration of hybrid models for DoS detection. - Lack of comprehensive evaluation on diverse datasets.
[7]	2023	Awatef Balobaid, Saahira Ahamed, Shermin Shamsudheen, S Balamurugan.	- Clustering and routing algorithms based on neural networks. - Particle swarm optimization for routing efficiency. - Random forest algorithm for intrusion detection classification.	-Accuracy - 90%, -Specificity – 0.93 -Sensitivity - 0.93 -Significant increase in network lifetime and performance observed. - Swarm intelligence provides high flexibility and efficiency.	- Need for improved event detection algorithms using machine learning. - Lack of real-time data application for enhanced efficiency. - Limited reliability of machine learning predictions without historical data.

[8]	2023	Ruqaya Alhasan, Ekhlas Kadhum	-Convolutional Neural Networks (CNNs) for intrusion detection. - PCA for dimensionality reduction. - SVD for feature extraction.	-IDS-CNN achieved 99.66% accuracy on UNSW-NB15 dataset and 99.26% accuracy on WSN-DS dataset.	-Existing methods have low detection rates in WSNs. - High computational overhead affects intrusion detection performance. - False alarms are prevalent in current intrusion detection systems.
[9]	2023	- Qaiser Abbas, Sadaf Hina, Hamza Sajjad, Shabih Khurram, Zaidi, Rehan Akbar, Wenbing Zhao.	-Data normalization technique was utilized for input data. -Wrapper-based feature elimination method selected important features. - RF-RFE, MLP, Random Forest, and SVM used for modelling hybrid ensemble model.	- The proposed model achieved 99% accuracy on NSL-KDD, 98.53% accuracy on UNSW-NB15 dataset and 99.9% accuracy on CSE-CIC-IDS2018 dataset.	-Need for comprehensive real-world attack datasets. -Challenges in deploying models on resource-constrained devices. - Imbalance in datasets affecting performance on minority classes.
[10]	2023	Thanh-Huy Nguyen, Van Nguyen, Thai Tung, Tran Dung, Le Thi, Thanh Thuy, Nguyen Liem Hieu, Minh Nguyen, Dung, Nguyen Van Ba.	- Use of diverse datasets for improved detection. - Implementation of transfer learning techniques.	- ANN accuracy 91%, LSTM accuracy 74%, and CNN accuracy 83%. - LSTM and CNN showed good performance with time series data.	- Limited dataset representation affects accuracy and detection rates. - Outdated datasets may lead to incorrect evaluations. - Need for complete and diverse data for effectiveness.
[11]	2023	C. Murugesh, S. Murugan	-Moth Search Optimizer (MSO) for hyper-parameter tuning. -Convolutional Recurrent Neural	MSODL-ID accuracy - 99.72%. Sensitivity - 95.67% Specificity-	-Difficulty in enhancing recognition performance of IDS. -High false alarm

			Network (CRNN) for intrusion detection. -Min-max normalization for feature extraction.	99.39%.	rates in current intrusion detection systems.
[12]	2023	Yu Yang, Yuheng Gu, Yu Yan.	-Geometric synthetic minority oversampling technique (G-SMOTE) for rare-class data. -Multiple denoising autoencoders (MDSAE) for feature extraction. -Random Under-Sampling (RUS) for majority class data.	- The model achieved 86.39% accuracy on NSL-KDD dataset and 99.94% accuracy on N-BaIoT dataset. - The model outperformed other advanced intrusion detection models.	- Traditional classifiers struggle with imbalanced attack distributions. - Existing methods do not address high-dimensional class imbalance effectively.
[13]	2023	Vishwanadham Mandala, T Senthilnathan, S Suganyadevi, S Gobhinath, Dhanasekaran Selvaraj, R Dhanapal.	-Optimized Back Propagation Neural Network (OBPNN) technique is utilized. -Fish Swarm Algorithm (FSA) optimizes the SVM. -Kernel density estimation removes outliers from data.	- The OBPNN technique shows improved fault extrapolation capabilities. - High precision rate of 97% compared to existing methods. - Effective health score calculation for monitoring engine subsystems.	- Limited information on actual failures in maintenance. - Challenges in modeling typical behavior from condition monitoring data. - Skewed class distribution in machine data complicates fault diagnosis.
[14]	2023	Vaishnavi Sivagaminathan, Manmohan Sharma, Santosh Kumar.	- Feature selection by PSO. - Various ML models trained, including ANN and KNN. - Wireshark used for data packet collection.	- PSO + ANN demonstrated the lowest false positive rate. - Predictability for PSO + ANN was 99.7%.	- Limited exploration of advanced machine learning algorithms is noted.

[15]	2023	Albara Awajan	- A four-layer CNN architecture is utilized. - Loss function - Gradient Descent – Back propagation algorithm updates weights of hidden nodes.	Accuracy 93.74%. Precision 93.71%, Recall 93.82% F1-score 93.47%.	- The system lacks comparison with other published methodologies. - Requires retraining for every new IoT network deployment.
[16]	2023	S. Santhosh Kumar, M. Selvi, A. Kannan	- The paper surveys existing intrusion detection systems (IDS). - It proposes a new intelligent IDS using deep learning. - Hybrid methods combine anomaly detection and signature generation.	- Security is enhanced - Network lifetime is increased - Detection accuracy is enhanced	- Most existing IDSs are generic and focus on network security. - Limited use of DL for reliable ID. - Existing approaches involve high computational complexities and overheads.
[17]	2023	D Govindaraj, B Jayanthi	- Optimal Support Vector Machine (OSVM) for intrusion classification. -Whale Optimization Algorithm (WOA) for kernel discovery in SVM.	Accuracy-95.02% - The false detection rate was minimized significantly. - The proposed architecture is lightweight and efficient.	- Limited exploration of trust-based IDS effectiveness in diverse WSNs. - Lack of comprehensive evaluation of routing protocols' security.
[18]	2023	Avinash Bhagat, Manmohan Sharma, Ajay Kushwaha, Shilpa Sharma, Hussien Sobahi.	-NN-LEACH protocol for energy optimization in WSN. -Mote clustering for energy efficiency and performance. - Optimum routing for data transmission.	-NN-LEACH outperforms GAECH, GCA, EAERP, and LEACH. -Higher residual energy observed in proposed LEACH. - More packets sent to base station with NN-LEACH.	- The study lacks comprehensive evaluation of energy optimization methods. - Limited exploration of multi-target enhancement concerns in WSNs.

[19]	2023	B Kannan, S Srinivasan	- Energy Efficient Intrusion Detection System (EE-IDS) is proposed. - Watchdog nodes monitor packet transmission timings. - Hidden Markov Model (HMM) estimates energy consumption.	- The proposed EE-IDS outperforms existing methods in DDoS detection. - EE-IDSEP shows superior performance compared to current EE-TS.	-Current security measures consume excessive energy and resources. - Need for lightweight, energy-efficient IDS for constrained networks.
[20]	2022	Fuad Owaimer, Ayman Tanira, Mohammed Hatab, Mohammad Mikki, Abu Fuad, Ayman Owaimer, Mohammed Tanira, Mohammad Hatab.	-Combination of anomaly-based and signature-based intrusion detection methods. - Cluster head selection management by base station - Sensor nodes monitor traffic and report suspicious activities.	- The proposed IDS shows acceptable performance compared to other hybrid IDSs. - Costs on the cluster head communication are reduced. - The lifetime of the entire WSN is improved.	- Future research on machine learning for IDS is suggested. - Reinforcement learning techniques could enhance detection accuracy. - Limited exploration of network attack detection methods is noted.
[21]	2022	Abhilash Singh, J Amutha, Jaiprakash Nagar, Sandeep Sharma, Cheng-Chi Lee.	- AutoML for model selection and hyperparameter optimization. -Monte Carlo simulation for synthetic predictor generation. -Bayesian optimization for hyperparameter tuning.	- Gaussian process regression outperforms other models with R = 1. - Model achieved RMSE of 0.007 and bias of -0.006. - Performance on public dataset: R = 0.92, RMSE = 30.59.	- Sensor aging may degrade model performance over time. - AutoML approach may struggle with dynamic datasets.

[22]	2021	Jing Jin	- Multicorrelation-based ID model for WSN. - Information gain feature selection algorithm for high dimensionality data. -Feature extraction through Bidirectional LSTM network. - C5.0 classifier for training and classification.	- High Detection rates for DOS and Probing attacks. - Low Detection rates for U2R and R2L attacks. - False alarm rates can reach up to 19.85%. -BiLSTMC5.0 model outperforms other classifiers in accuracy.	- Limited detection rates for U2R and R2L attacks. - High dimensionality of intrusion detection data sets remains challenging. - Misjudgements due to small data amounts in certain attack types.
[23]	2023	Vanlalruata Hnamte, Jamal Hussain.	- Deep CNN-BiLSTM - Utilization of CICIDS2018 and Edge_IIoT datasets for training. - Implementation of Conv1D and Bidirectional LSTM layers.	- DCNNBiLSTM model achieved 100% detection accuracy. - The model was trained on CICIDS2018 and EdgeIIoT datasets.	- Existing IDS designs have low overall performance. - Imbalanced datasets affect classification accuracy. - Longer training periods due to model complexity.

From the above study, the complexity in identification of the attacks in WSN is spotted out and also reveals the critical areas for further exploration. This not only contextualizes the study but also emphasizes the necessity of the continuous investigation to be carried out.

5. Identification of research gap

- Optimization Techniques for Resource-Constrained Environments: While optimization-driven machine learning models have shown promise in attack detection, the unique resource limitations of WSNs necessitate tailored methods. Research is needed to create lightweight optimization strategies that can operate effectively on sensor nodes with restricted computing power, memory, and energy.
- Adaptive Ensemble Models: Existing ensemble models often use fixed combinations of algorithms. There exists a research gap in framing adaptive ensemble models that are capable of modifying their architecture and weighting dynamically in response to changing threat

landscapes and inconsistent network conditions. This kind of adaptability could improve the resilience and longevity of WSN attack detection systems significantly.

- Feature Selection and Dimensionality Reduction: Although this domain is esteemed for its potential, a thorough research into the ramifications of feature selection and dimensionality reduction on ML model performances for WSN attack detection are alarmingly limited. Further research should be concentrated on identifying the most efficient approaches to refine the input space without jeopardizing or elevating the detection precision.
- Real-Time Learning and Adaptation: There are numerous models built for offline use, which restricts their ability to swiftly adjust to new attacks. It is very essential to develop real-time learning strategies that can refresh models dynamically without significant computational costs, ensuring the system is robust against identifying new threats.

6. Aim

The main objective of this research is the design and evaluation of a hybrid machine learning model along with a novel ensemble technique for efficient detection and classification of network threats in the Wireless Sensor Networks (WSNs). This investigation strives to attain superior accuracy and reliability, ensuring that the developed model exceeds the performance of the existing conventional methods based on different vital performance metrics such as precision, recall, accuracy, and error rate.

7. Objectives

- To design and evaluate a hybrid machine learning model to detect WSN attacks.
- To design and implement a novel ensemble model to detect the various threats in WSNs.
- To evaluate the performance of the proposed models.
- To conduct a comparative analysis with the other reported techniques.
- To identify the strengths and limitations.
- To establish a benchmark for future research.

8. Research Questions

- How effective is the hybrid ML model and novel ensemble model in detecting and classifying network attacks in Wireless Sensor Networks compared to existing classifiers?
- What is the impact of integrating the optimization technique and ML model?
- What is the impact of combining the weak-weak learner and strong-strong learners?
- What are the strengths and limitations of the proposed methodologies in minimizing false positives and false negatives for network traffic classification?

9. Methodology

A. Literature Review

- Problem statement
- Literature Review
- Research gap
- Aim and objectives

B. Data Collection and Preparation

- Identification of source for data collection
- Feature Importance

C. Data Preprocessing

- Data Normalization
- Noise Filtering
- Handling Imbalanced Data

D. Model Development

- Building of Layers
- Training Configuration

E. Model Deployment

- Training the network using training data
- Testing the model using test data
- Evaluation of Performance Metrics

F. Comparative Analysis

- Comparing the results of the proposed methodology with the reported methods
- Visualization of the results

G. Discussion and Future work

- Limitations and Enhancements
- Scalability

References

[1] M. Alshinwan et al., "Enhanced Prairie Dog Optimization with Differential Evolution for solving engineering design problems and network intrusion detection system," Heliyon, vol. 10, no. 17, p. e36663, 2024, doi: 10.1016/j.heliyon.2024.e36663.

[2] G. Nagalalli and G. Ravi, "A Novel MegaBAT Optimized Intelligent Intrusion Detection System in Wireless Sensor Networks," Intell. Autom. Soft Comput., vol. 35, no. 1, pp. 475–490, 2023, doi: 10.32604/iasc.2023.026571.

[3] A. Gautami, J. Shanthini, and S. Karthik, “A Quasi-Newton Neural Network Based Efficient Intrusion Detection System for Wireless Sensor Network,” Comput. Syst. Sci. Eng., vol. 45, no. 1, pp. 427–443, 2023, doi: 10.32604/csse.2023.026688.

[4] M. Aljebreen et al., “Binary Chimp Optimization Algorithm with ML Based Intrusion Detection for Secure IoT-Assisted Wireless Sensor Networks,” Sensors, vol. 23, no. 8, 2023, doi: 10.3390/s23084073.

[5] M. Karthikeyan, D. Manimegalai, and K. RajaGopal, “Firefly algorithm based WSN-IoT security enhancement with machine learning for intrusion detection,” Sci. Rep., vol. 14, no. 1, 2024, doi: 10.1038/s41598-023-50554-x.

[6] S. Salmi and L. Oughdir, “Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network,” J. Big Data, vol. 10, no. 1, 2023, doi: 10.1186/s40537-023-00692-w.

[7] A. T. Azar, E. Shehab, A. M. Mattar, I. A. Hameed, and S. A. Elsaid, Deep Learning Based Hybrid Intrusion Detection Systems to Protect Satellite Networks, vol. 31, no. 4. Springer US, 2023. doi: 10.1007/s10922-023-09767-8.

[8] R. A. Alhasan and E. K. Hamza, “A Novel CNN Model with Dimensionality Reduction for WSN Intrusion Detection,” Rev. d’Intelligence Artif., vol. 37, no. 5, pp. 1121–1131, 2023, doi: 10.18280/ria.370504.

[9] Q. Abbas, S. Hina, H. Sajjad, K. S. Zaidi, and R. Akbar, “Optimization of predictive performance of intrusion detection system using hybrid ensemble model for secure systems,” PeerJ Comput. Sci., vol. 9, 2023, doi: 10.7717/peerj-cs.1552.

[10] S. Darla and C. Naveena, “An Optimized Deep Learning Based Malicious Nodes Detection in Intelligent Sensor-Based Systems Using Blockchain,” J. Adv. Inf. Technol., vol. 14, no. 5, pp. 1037–1045, 2023, doi: 10.12720/jait.14.5.1037-1045.

[11] C. Murugesh and S. Murugan, “Moth Search Optimizer with Deep Learning Enabled Intrusion Detection System in Wireless Sensor Networks,” SSRG Int. J. Electr. Electron. Eng., vol. 10, no. 4, pp. 77–90, 2023, doi: 10.14445/23488379/IJEEE-V10I4P108.

[12] Y. Yang, Y. Gu, and Y. Yan, “Machine Learning-Based Intrusion Detection for Rare-Class Network Attacks,” Electron., vol. 12, no. 18, 2023, doi: 10.3390/electronics12183911.

[13] G. G. Gebremariam, J. Panda, and S. Indu, “Design of advanced intrusion detection systems based on hybrid machine learning techniques in hierarchically wireless sensor networks,” Conn. Sci., vol. 35, no. 1, 2023, doi: 10.1080/09540091.2023.2246703.

[14] V. Sivagaminathan, M. Sharma, and S. K. Henge, “Intrusion detection systems for wireless sensor networks using computational intelligence techniques,” Cybersecurity, vol. 6, no. 1, 2023, doi: 10.1186/s42400-023-00161-0.

[15] A. Awajan, “A Novel Deep Learning-Based Intrusion Detection System for IoT Networks,” Computers, vol. 12, no. 2, 2023, doi: 10.3390/computers12020034.

[16] S. V. N. Santhosh Kumar, M. Selvi, and A. Kannan, “A Comprehensive Survey on Machine Learning-Based Intrusion Detection Systems for Secure Communication in Internet of Things,” Comput. Intell. Neurosci., vol. 2023, pp. 1–24, 2023, doi: 10.1155/2023/8981988.

[17] R. Wazirali and R. Ahmad, “Machine learning approaches to detect DoS and their effect on WSNs lifetime,” Comput. Mater. Contin., vol. 70, no. 3, pp. 4921–4946, 2022, doi: 10.32604/cmc.2022.020044.

[18] A. Singh, J. Amutha, J. Nagar, S. Sharma, and C. C. Lee, “AutoML-ID: automated machine learning model for intrusion detection using wireless sensor network,” Sci. Rep., vol. 12, no. 1, pp. 1–14, 2022, doi: 10.1038/s41598-022-13061-z.

[19] A. Bouazza, H. Debbi, and H. Lakhlef, “Machine Learning-based Intrusion Detection System Against Routing Attacks in the Internet of Things,” CEUR Workshop Proc., vol. 3333, pp. 45–56, 2021.

[20] J. Karthika, S. Loganathan, and M. Vanathi, “A Hybrid Machine Learning Based Feature Selection Technique for Attack Detection in NIDS,” J. Phys. Conf. Ser., vol. 2335, no. 1, 2022, doi: 10.1088/1742-6596/2335/1/012033.

[21] M. Zang and Y. Yan, “Machine Learning-Based Intrusion Detection System for Big Data Analytics in VANET,” IEEE Veh. Technol. Conf., vol. 2021-April, pp. 1–5, 2021, doi: 10.1109/VTC2021-Spring51267.2021.9448878.

[22] M. A. Khan et al., “A deep learning-based intrusion detection system for mqtt enabled iot,” Sensors, vol. 21, no. 21, pp. 1–25, 2021, doi: 10.3390/s21217016.

[23] J. Jin, “Intrusion Detection Algorithm and Simulation of Wireless Sensor Network under Internet Environment,” J. Sensors, vol. 2021, 2021, doi: 10.1155/2021/9089370.

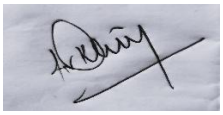
[24] J. Lansky et al., “Deep Learning-Based Intrusion Detection Systems: A Systematic Review,” IEEE Access, vol. 9, pp. 101574–101599, 2021, doi: 10.1109/ACCESS.2021.3097247.

[25] I. Idrissi, M. Azizi, and O. Moussaoui, “A Lightweight Optimized Deep Learning-based Host-Intrusion Detection System Deployed on the Edge for IoT,” Int. J. Comput. Digit. Syst., vol. 11, no. 1, pp. 209–216, 2022, doi: 10.12785/ijcds/110117.

Signature:

Date: 07/03/2025

Name of Scholar: Ms. Divya Bhavani Mohan

Signature: 

Date: 07/03/2025

Name of Guide: Dr. Prakash Arumugam